Claims

1. Method for operating a data processing system with copy protection for user programs, whereby the data processing system can be directly connected to a copy protection identification (KI_D) via a hardware module, comprising the following steps:

(a) a plurality of application [sic] programs as well as an installation program and a cryptoprogram are on hand on a storage medium (CDROM) intended for the user,

(b) a user identification (AI) that identifies the user, an encrypted product identification (PI) that references at least one user program and a copy protection identification (KI_E) are communicated to the user, whereby the communicated copy protection identification (KI_E) corresponds to the copy protection identification (KI_D) connected via the hardware module,

(c) when processing the installation program on the data processing system, the communicated copy protection identification (KI_E), the user identification (AI) and the product identification (PI) are input,

(c1) each user program contains a predetermined memory area into which the copy protection identification (KI) can be entered,

(c2) the installation program compares the copy protection identification (KI_E) that has been input to the copy protection identification (KI_D) connected with the hardware module and, given coincidence, deciphers the encrypted product identification (PI) upon utilization of the user identification (AI) as key, and identifies the user program referenced in the product identification (PI),

(c3) the selected user program is loaded from the storage medium (CDROM) into a memory area of the data processing system,

(c4) the cryptoprogram enters the copy protection identification (KI) into the predetermined memory area of the selected user program,

and whereby

(d) before the running of the selected application [sic] program, the copy protection identification (KI) contained in the predetermined memory area is compared to the copy protection identification (KI_D) directly connected with the data processing system via the hardware module, and the user program is run only given coincidence.

2. Method according to claim 1, characterized in that, when running the installation program, further running of the installation program is only continued after the comparison of the copy protection identification (KI_E) that has been input to the copy protection identification (KI_D) connected with the data processing system given coincidence.

3. Method according to claim 1 or 2, characterized in that the product identification (PI) also contains the copy protection identification (KI_{PI}), and in that this copy protection identification (KI_{PI}) is compared to the copy protection identification (KI_D) connected with the data processing system, and the running of the further program steps is continued only given coincidence.

4. Method according to one of the preceding claims, characterized in that the product identification (PI) references a plurality of application [sic] programs; in that a list of these application [sic] programs is determined upon decipherment of the product identification (PI); and in that this list is checked for correctness.

5. Method according to claim 1, characterized in that the check of the list for correctness ensues on the basis of a checksum check.

6. Method according to one of the preceding claims, characterized in that the user makes a selection from the application [sic] programs of the list; and in that only the selected application [sic] programs are loaded from the storage medium into the memory area of the data processing system.

7. Method according to one of the preceding claims, characterized in that an authentification between the installation program and the key program is undertaken when the key program is called.

8. Method according to claim 7, characterized in that the authentification is implemented according to the known challenge-response protocol.

9. Method according to one of the preceding claims, characterized in that the product identification is compressed according to the static Huffman-Baum method.

10. Method according to one of the preceding claims, characterized in that the copy protection identification (KI_D) connected with the data processing system is

situated on a hardware module that is permanently connected to the data processing system.

11. Method according to claim 11 [sic], characterized in that the hardware module is a dongle that is pluggably connected to a parallel or to a serial interface or to a USB bus of the data processing system; and in that this dongle contains the copy protection identification (KI_D)